UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,975	08/04/2003	Yuying Ding	9-16654-1US	2994

7590 11/03/2006

Yuying Ding
Rm 302 100 Zhengde East Rd
Yangpu District
Shanghai, 200433
CHINA

EXAMINER	
RUSSELL, TRACI L	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/632,975	DING, YUYING	
	Examiner	Art Unit	
	Traci L. Russell	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 August 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/04/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Pursuant to USC 131, claims 1- 26 have been examined.

Information Disclosure Statement

Examiner acknowledges receipt of Information Disclosure Statement. IDS has been recorded and considered in the examination.

Drawings

1. The drawings are objected to because of incorrect variables and inconsistent flow illustrated. In figure 2, the "secure header 26" and "code message 28" are missing. In figure 3, the "encrypted code 22" is misnumbered. In figure 4, no numbering or clear flow illustrated in the drawing. In figure 8, inconsistent flow is illustrated. Corrected drawing sheets in compliance with 37 CFR 1.121(d) is required in reply to the Office action to avoid abandonment of the application. Any amended replacement-drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the change is not accepted by the examiner, the

applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 9 recites the limitation "said binary transformation module". There is insufficient antecedent basis for this limitation in the claim. Furthermore, the binary transformation module is not disclosed in claim 6. The module is disclosed in claim 7. Appropriate correction is required.

4. Claim 15 discloses the "normalized inner product" of the decryption orthogonal code and received message. "normalized inner product" lacks definition and is unclear what constitutes the "normalized inner product" in the claim. For the purpose of examination, the examiner interprets 'normalized inner product' as the product of the decrypted code and the received message. Appropriate correction is required.

5. Claim 23 discloses "encrypting acknowledgements" and "broadcasting an acknowledgement message" which limits the claim as indefinite. For the purpose of examination, the examiner interprets acknowledgement as broadcasting. Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1- 26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

7. Functional descriptive material, per se is not statutory. However, functional descriptive material claimed in combination with an appropriate computer readable medium to enable the functionality to be realized is patent eligible subject matter if it is capable of producing a useful, concrete, and tangible result.

8. Computer readable medium must be of a physical structure which provides the functional descriptive material in usable form to permit functionality to be realized with the computer.

9. A program product which does not explicitly include such a medium, a program per se, or other type of transmission media that fails to include the hardware necessary to realize the functionality, and a piece of paper with the functional descriptive material written on it are all examples of media which are not believed to enable the functionality to be realized with the computer. Appropriate correction is required.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section

351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1, 2, 4, 15-17 are rejected under 35 U.S.C. 102(e) as being unpatentable over George (US 2004/0203957).

(1) with regard to claims 1:

George discloses orthogonalization of messages using a communications device comprising orthogonal code [Page 1, paragraph 20; Page 3, paragraphs 49 and 50]. George also discloses a multi-casting communications device for secure communications (in a highly dynamic environment between members of a predefined communications group that includes a plurality of group members, comprising:

a code module ['central database'; Page 3, paragraph 46] for maintaining an code table ['orthogonalized message in partition...'; Page 3, paragraphs 46-50] by reciprocally exchanging code with a communications device operated by each new member that joins the group ['radio telecommunications system', 'group member user terminal'; Page 1, paragraph 8], and deleting from the table the orthogonal code associated with the communications device of any group member that leaves the group ['uplink of random access channel used to update information'; Page 4, paragraph 69];

an encryption module and decryption module for encrypting a message to be sent to one or more of the group members using the code associated with respective communications devices operated by the group members to which the message is to be sent operated by any of the other group members [each unit/member is capable of encryption [Page 2; paragraph 39] or decryption of messages; Page 2; paragraph 25].

In addition, each participant involved is defined in advance, interchanging information between them [Page 2; paragraph 23].

(2) with regard to claim 2:

George discloses a code generator module for generating the orthogonal codes ['orthogonalization'; Page 1; paragraphs 19 and 20].

(3) with regard to claim 4:

George discloses wherein said code module comprises an orthogonal generator for generating a set of orthogonal and pseudo random orthogonal codes that are of identical length ['randomization'; Page 1, paragraph 17; Page 3, paragraph 47].

(4) with regard to claim 15:

George discloses wherein said decryption module comprises a function for accessing to the orthogonal code table to obtain a decryption orthogonal code associated with the communications device operated by the group member who sent the message ['unique key is de-compressed; Page 3, paragraphs 54-55]; and a function for computing a normalized inner product of the decryption orthogonal code and the received message to decrypt the message [de-orthogonalize'; Page 3, paragraphs 56-57'].

(5) with regard to claim 16:

George discloses wherein said orthogonal code module comprises a function for sending an orthogonal code to each new group member and a function for confirming receipt of an orthogonal code by the new group member ['acknowledgement'; Page 4, paragraphs 68-69].

(6) with regard to claim 17:

George discloses wherein the function for sending orthogonal codes comprises means for encrypting respective orthogonal codes for a number of recipients, concatenating the encrypted orthogonal codes and broadcasting the concatenated orthogonal codes ['messages are grouped...'; Page 1, paragraphs 14-16].

12. Claims 18-22, and 25-26 are rejected under 35 U.S.C. 102(e) as being unpatentable over Hardjono (US 6,584,566).

(1) with regard to claim 18:

Hardjono discloses maintaining a table for each group member by reciprocally exchanging a key with each new member that joins the group ['common group key'; Col 7, lines 25-28], and deleting from the table the key associated with any group member that leaves the group ['group key is replaced'; Col 8, lines 14-18]; encrypting a message to be sent to one or more of the group members using the key associated with respective group members to which the message is to be sent ['encrypted key'; Col 7, lines 46-48]; and decrypting a message sent from a communications device operated by

any of the other group members ['multicasting'; Col 10, lines 40-46].

(2) with regard to claim 19:

Hardjono discloses exchanging a key with each new member that joins the group further comprises encrypting the key prior to sending the key to the new member ['membership change'; Col 7, line 67 and Col 8, lines 1-3].

(3) with regard to claim 20:

Hardjono discloses wherein the encrypting comprises encrypting each key using one of: symmetric encryption if a sender of the orthogonal code has a pre-arranged shared symmetric key with the recipient, and otherwise using public key encryption with a public key of the recipient ['cipher key code'; Page 1, paragraph 18].

(4) with regard to claim 21:

Hardjono discloses wherein said pre-arranged shared symmetric key is exchanged offline between the two parties before the secure group communication occurs ['secure association is not always distributed with key....'; Col 11, lines 10-24].

(5) with regard to claim 22:

Hardjono discloses wherein the public key is obtained from a directory service ['key server'; Col 4, lines 31-35].

(6) with regard to claim 25:

Hardjono discloses wherein when a member leaves the group, the method further comprises: deleting the encryption code assigned to said leaving member; deleting the decryption code assigned by said leaving member; and deleting an identity of the leaving member from a group members list ['member leaving'; Col 8, lines 10-18].

(7) with regard to claim 26:

Hardjono discloses a method wherein when a new member joins the group, the method further comprises sending a join request to all group members with which the new member desires secure communications ['member join/rekey'; Col 5, lines 23-26]; receiving a refusal acknowledgment from each group member that does not desire secure communications with the new member. Because of the secure connection, the refusal is interpreted by the examiner as being inherented; exchanging codes with each group member that accepts communications with the new member ['common key'; Col 7, lines 25-30]; and updating the orthogonal code table as the orthogonal codes are received from other group members ['member joining'; Col 10, lines 1-44].

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 3, 5 - 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over George (US 2004/0203957) in view of Hardjono (US 6,584,566).

(1) with regard to claim 3:

George discloses all the information as being claimed in claim 1. However, Hardjono discloses a message amalgamating module for amalgamating a number of messages addressed to other group members into an amalgamated message ['multicast messaging; Col 10, lines 40-44].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the device as disclosed by George to include imalgamation as disclosed by Hardjono in order to increase security and to produce an efficient single message size among group members [Col 10, lines 44-46].

(2) with regard to claim 5:

George discloses all the information as claimed in claim 1. However, Hardjono discloses wherein said orthogonal code table comprises a group member list, an encryption orthogonal code list, a decryption orthogonal code list and an unused orthogonal code list ['key server'; Col 4, lines 20-33].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made for George to include an orthogonal code table as disclosed by Hardjono in order to distribute keys to group members [Col 3, lines 17-26].

(3) with regard to claim 6:

George discloses all the information as claimed in claim 3. However, Hardjono discloses a message amalgamating module comprises a plurality of adders that output an amalgamated message by adding together encrypted messages addressed to a plurality of group members encrypted using respective encryption orthogonal codes associated with communications devices operated by the group members to which the respective messages are addressed ['key server'; Page 4, lines 20-33].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the device disclosed by George to include imalgamation as disclosed by Hardjono in order to increase security and to produce an efficient single message size [Col 10, lines 44-46].

(4) with regard to claim 7:

George discloses wherein said encryption module comprises an orthogonal code transformation function ['orthogonalization'; Page 1, paragraph 19], a binary transformation module ['bit-wise X-OR operation'; Page 2, paragraph 40], and an encryption function ['message is encrypted'; Page 2, paragraph 39].

(5) with regard to claim 8:

George discloses wherein said orthogonal code transformation function transforms an encryption orthogonal code to bipolar form in which each orthogonal code `1` is converted to `+1`, and each orthogonal code `0` is converted to `-1`['message is

orthogonalized'; Page 3, paragraph 49].

(6) with regard to claim 9:

George discloses wherein said binary transformation module transforms the messages into a binary format ['bit-wise X-OR operation'; Page 2, paragraph 40].

(7) with regard to claim 10:

George discloses wherein the encryption function accepts the message in binary format as input, examines each bit of the message and substitutes the bit with the encryption orthogonal code when the bit is "1" and a negative of said orthogonal code when the bit is "0" ['orthogonalized'; Page 3, paragraph 49].

(8) with regard to claim 11:

George discloses all the information as claimed in claim 10. However, Hardjono discloses wherein a plurality of encryption functions work in parallel so that a number of messages are encrypted concurrently ['re-keying' in Fig 5; Col 8, lines 34-60].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made for George to include parallel encryption as disclosed by Hardjono in order to reduce latency of re-keying to its members ['latency'; Col 8, lines 26-29].

(9) with regard to claim 12:

George discloses wherein the plurality of adders comprise parallel adders and a combining adder for combining outputs of the plurality of parallel adders ['data is added'; Page 3, paragraph 41].

(10) with regard to claim 13:

George discloses wherein the parallel adders add the encrypted messages bit by bit in parallel, and output the sum to the combining adder ['final fixed or dynamic compression'; Page 3, paragraph 41].

(11) with regard to claim 14:

George discloses wherein the combining adder accepts the outputs of the parallel adders and adds the accepted outputs bit by bit to generate the amalgamated message [message is combined'; Page 3, paragraph 50-51].

(12) with regard to claim 23:

Hardjono discloses all the information as claimed in claim 18. However, George discloses a step of confirming the exchange of orthogonal codes comprising collecting all orthogonal codes sent during a predetermined period of time ['acknowledgement'; Page 4, paragraphs 68-69]; encrypting acknowledgements using the an encryption module, and broadcasting a resulting amalgamated encrypted acknowledgement message ['encryption and broadcasting'; Page 1, paragraphs 14-16].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the method disclosed by George to include the method disclosed by Hardjono in order to increase security and to produce an efficient single message size among group members [Col 10, lines 44-46].

(13) with regard to claim 24:

Hardjono discloses all the information as claimed in claim 18. However, George discloses periodically generating a new set of orthogonal codes using an orthogonal code generating module ['orthogonalization'; Page 1, paragraphs 19-20]; assigning said new set of orthogonal codes, encrypting and amalgamating the assigned orthogonal codes to form a new code message, and sending the new code message to the other group members ['messages are grouped'; Page 1, paragraphs 14-16]; and recording the update in related orthogonal code tables ['uplink...'; Page 4, paragraph 69].

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the method disclosed by George to include the method disclosed by Hardjono in order to increase security and to produce an efficient single message size among group members [Col 10, lines 44-46].

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Traci L. Russell whose telephone number is

571.270.1095. The examiner can normally be reached on Mon - Fri (alternate Fridays off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571 272.4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Traci L. Russell
TLR

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/01/06